



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHIED	33012/274/10	4721

7590 10/08/2003

CHARLES A JOHNSON  
UNISYS CORPORATION  
LAW DEPARTMENT M S 4773  
2470 HIGHCREST ROAD  
ROSEVILLE, MN 55113

EXAMINER

WASSUM, LUKE S

ART UNIT PAPER NUMBER

2177

DATE MAILED: 10/08/2003

//

Please find below and/or attached an Office communication concerning this application or proceeding.

11

# Office Action Summary

Application No.

09/448,154

Applicant(s)

GERMSCHIED ET AL.

Examiner

Luke S. Wassum

Art Unit

2177

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 29 August 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 April 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### *Response to Amendment*

1. The Applicants' amendment, filed 29 August 2003, has been received, entered into the record, and considered.
2. As a result of the amendment, claims 1-3, 6, 8, 11 and 12 have been amended. Claims 1-20 remain pending in the application.
3. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

As such, the previous Office action is being treated as a non-final action, and the Applicants' amendment has been entered as a matter of right.

### *Drawings*

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description:

On replacement pages 33 and 34 of the specification, the Applicants cite with reference to Figure 10 the Cool ICE Engine Interface 331. However, in Figure 10, the Cool ICE Engine Interface does not include a reference number 331.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

*Specification*

5. Applicant has incorporated by reference numerous co-pending applications cited on replacement pages 1 and 2 et seq. of the specification. Examiner notes that incorporation by reference of an application in a printed United States Patent constitutes a special circumstance under 35 U.S.C. § 122 warranting that access of the original disclosure of the application be granted. The incorporation by reference will be interpreted as a waiver of confidentiality of only the original disclosure as filed, and not the entire application file. See *In re Gallo*, 231 USPQ 496 (Comm'r Pat. 1986).

If Applicant objects to access to the entire application file, two copies of the information incorporated by reference must be submitted along with the objection. Failure to provide the material within the period provided will result in the entire application (including prosecution) being made available to petitioner. The Office will not attempt to separate the noted materials from the remainder of the application. See *In re Marsh Engineering Co.*, 1913 C.D. 183 (Comm'r Pat. 1913).

6. In view of the Applicants' amendment to the specification, the objection based on the presence of hypertext in the specification is withdrawn.

7. The disclosure is objected to because of the following informalities:

The terms "User Validation Service" and "UserID/Password" are used in the specification to refer to different things. This fact renders relevant portions of the specification indefinite.

For instance, on page 7, lines 9-11, it is disclosed that the user signs in by entering a UserID and Password, which the examiner will refer to as the user-specific UserID and Password. Later, at lines 12-14, it is disclosed that site-specific data is converted to a valid UserID and Password, which

Art Unit: 2177

the examiner will refer to as site-specific UserID and Password. Further still, at lines 17-19, it is disclosed that 'information' is translated into a UserID and Password, which the examiner will refer to as the server UserID and Password. The use of these terms to refer to multiple instances adds confusion to the specification.

Similarly, on page 7, lines 12-15, the specification discloses the use of a User Validation Service resident on the client terminal ("the site") which will convert site-specific data to a valid UserID/Password (the site-specific UserID and Password). Further, at lines 17-19, it is disclosed that a User Validation Service resident on the Cool ICE server will convert "information" (the site-specific UserID/Password) to a UserID/Password (the server UserID and Password). Once again, the use of a single term when referring to different things adds confusion to the specification.

Furthermore, there appear to be inconsistencies in the disclosure of the invention.

On page 7, lines 12-16, it is disclosed that the client site contains "site-specific data" that can be used to identify a user. A User Validation Service running on the client site terminal converts this site-specific data to a valid UserID/Password (the site-specific UserID/Password).

At lines 17-20 it is disclosed that on the Cool ICE server, another User Validation Service converts "information" (presumably the site-specific UserID/Password) to a UserID/Password (the server UserID/Password). The examiner assumes that the "information" comprises the site-specific UserID/Password, since there appears to be no other reason for the User Validation Service on the client site to convert the "site-specific data" to a site-specific UserID/Password if this is not the case.

The inconsistency is that on page 7, lines 19-20, it is disclosed that the invention precludes the need to send a UserID/Password from the browser to the server, but as stated above, the site-

Art Unit: 2177

specific UserID/Password is indeed passed from the browser to the server. Furthermore, on replacement page 34, lines 9-12, it is disclosed that the service handler requests the user to provide a UserID, and that UserID is transmitted via the Internet to the server, where it is compared to the security profile of a requested script.

Given these facts, there is inconsistency between the claimed feature of the invention (that no UserID/Password is transmitted from browser to server via the Internet) and the disclosed details of the invention (that the User Validation Service resident on the site converts the site-specific data to site-specific UserID/Password, which is passed to the server; and also that a service handler resident on the server requests the user to provide a UserID, and that UserID is transmitted via the Internet to the server, where it is compared to the security profile of a requested script).

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Art Unit: 2177

10. Regarding claims 1, 6, 11 and 16, the claim limitations of the independent claims regarding the use of a site specific security profile in permitting access to a database without requiring the transfer of a user identifier via a publicly accessible digital data communications network are discussed in the Summary of the Invention, pages 7-9. However, the details of the use of the site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed. This disclosure is inconsistent with the claim language. The lack of a detailed disclosure of the claimed invention renders the invention non-enabled.

11. Claims 2-5, 7-10, 12-15 and 17-20 are also rejected as being non-enabled, inheriting the deficiencies of their parent independent claims, and furthermore because other claimed details, such as the "special field" of claims 3, 7, 13 and 17, and the mechanism for the generation of the site specific security profile by the database management system (claims 3 and 6), are not disclosed in the specification.

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2177

13. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claim language, as discussed above with regard to 35 U.S.C. 112 first paragraph, is inconsistent with the disclosure of the invention. This inconsistency renders the claims indefinite, in accordance with MPEP § 2173.03[R-1]:

"Although the terms of a claim may appear to be definite, inconsistency with the specification disclosure or prior art teachings may make an otherwise definite claim take on an unreasonable degree of uncertainty. In *re Cohn*, 438 F.2d 989, 169 USPQ 95 (CCPA 1971); In *re Hammack*, 427 F.2d 1378, 166 USPQ 204 (CCPA 1970). In *Cohn*, the claim was directed to a process of treating a surface with a corroding solution until the metallic appearance is supplanted by an "opaque" appearance. Noting that no claim may be read apart from and independent of the supporting disclosure on which it is based, the court found that the description, definitions and examples set forth in the specification relating to the appearance of the surface after treatment were inherently inconsistent and rendered the claim indefinite."

### *Claim Rejections - 35 USC § 103*

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.



Art Unit: 2177

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

17. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems").

18. Regarding claim 1, **Garrison** teaches a data processing environment having a user terminal at a site for generating a service request responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database as claimed, comprising security profile corresponding to a site whereby said database management system permits said user terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

**Garrison** does not explicitly teach a data processing environment wherein the security profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see Yoshimoto, col. 6, lines 15-21).

Neither Garrison nor Yoshimoto explicitly teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is,

Art Unit: 2177

remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

19. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

- a) a user terminal located at a site (see col. 4, lines 1-32);
- b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and
- c) a security profile generated by said database management system corresponding to said site whereby said database management system provides access to a particular portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

**Garrison** does not explicitly teach an apparatus wherein the security profile is site-specific.

**Yoshimoto**, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

**De Capitani di Vimercati et al.**, however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect

all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

20. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal having a user with a user identifier located at a site to access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

- a) signing on to said user terminal by said user utilizing said user identifier (see col. 2, line 64 through col. 3, line 2, disclosing that the client transmits a password to the client to identify the user of the client system, meaning that the user has necessarily signed on to the client system utilizing a user identifier);
- b) transmitting a service request requiring access to said database from said user terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
- c) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
- d) determining a security profile corresponding to said site (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);
- e) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and
- f) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

**Garrison** does not explicitly teach a method wherein the security profile is site-specific.

**Yoshimoto**, however, teaches a method wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

**De Capitani di Vimercati et al.**, however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is,

remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

21. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

- a) means located at a site for permitting a user to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);
- b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and
- c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

**Garrison** does not explicitly teach an apparatus wherein the security profile is site-specific.

**Yoshimoto**, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

**De Capitani di Vimercati et al.**, however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is,



Art Unit: 2177

remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

22. Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

23. Regarding claims 3, 8, 12, 13 and 18, **Garrison** additionally teaches an improvement, method and apparatus further comprising a special field responsively coupled to a service request whereby said database management system receives said special field and generates said security profile corresponding to said site and to said special field (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

24. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

25. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said user terminal accesses said data entity by transferring a service request to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

26. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **King** ("Hazards Control Department Use of the Sperry Database Management System MAPPER").

27. Regarding claims 5, 9, 15 and 19, **Garrison**, **Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison**, **Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **King** teaches a system wherein the database management system used is MAPPER (see first paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is extremely versatile and is considered one of the best fourth generation programs, and furthermore since it contains, in

addition to a database management system, a word processor, office automation program including electronic mail, and color graphics routines (see **King**, first paragraph).

28. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

29. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

30. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

31. Regarding claims 5, 9, 15 and 19, **Garrison**, **Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison**, **Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

32. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

33. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

34. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Gebauer** (U.S. Patent 6,324,539).

Art Unit: 2177

35. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto and De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Gebauer** teaches a system wherein the database management system used is MAPPER (see col. 1, lines 56-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is one of the most successful database management systems available (see **Gebauer**, col. 1, lines 56-65), and furthermore that providing access to a proprietary database management system such as MAPPER through the Internet would yield an extremely inexpensive and universally available means for accessing the data which it contains and such access would be without the need for considerable specialized training (see **Gebauer**, col. 2, lines 45-51).

36. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

37. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

### *Response to Arguments*

38. Applicants' arguments filed 29 August 2003 have been fully considered but they are not persuasive.

39. In response to the Applicants' arguments regarding the rejection of all claims under 35 U.S.C. § 112, first paragraph, the examiner responds that, as discussed above regarding the objection to the specification, there are inconsistencies between the claimed invention and the disclosure, which render the specification non-enabled.

Furthermore, the disclosure of a process for creating a site-specific security profile, comprising a single sentence in the specification and the drawing Figure 13, does not provide the details that an ordinary artisan would require in order to make and/or use the invention, as required by 35 U.S.C. § 112, first paragraph.

In particular, Figure 13 consists merely of a sequence of software module calls. Without any disclosure of what tasks the particular software modules perform, the drawing figure is non-enabling.

In response to the arguments regarding the rejections of the dependent claims, the examiner has once again examined the specification, and cannot find any disclosure of the "special field" cited in claims 3, 7, 13 and 17. On page 13 of the response, the Applicants cite a passage from page 8, lines 4-7 of the specification, which discloses the use of the "secret field". However, this passage

does not appear on page 8 of the specification, nor anywhere else. There is simply no disclosure of the claimed “special field”, nor any “secret field” anywhere in the specification.

The Applicants also directed the examiner’s attention to message # 2 of Figure 14, which reads in its entirety:

2. Call the ExtractSessionNumber method to extract a session number from the specified bstrSessionID parameter. The session number is used as an index for retrieve (sic) a CCISession object from the \_Module.m\_pSessions collection (sic).

The examiner respectfully submits that this teaching is not enabling of the claimed “special field responsively coupled to said service request”.

40. In response to the Applicants’ arguments regarding the rejection of all claims under 35 U.S.C. § 112, second paragraph, the rejections are maintained for the reasons cited above.

41. In response to the Applicants’ arguments regarding the combination of references in the rejections of the independent claims, the examiner does not find these arguments persuasive.

In particular, regarding the **De Capitini di Vimercati et al.** reference, it is taught on page 88, col. 2, section 2.1, that “in mandatory systems, where clearances are used in access controls instead of user identifiers, the user’s identity is needed to determine the security level with which the user can connect to the system”. The provision for entry of the user identifier in this case is completely analogous to the Applicants’ disclosure that the user must first sign into the user terminal using the user identifier (see claim 11, et seq.).

As is disclosed further down the column, “An alternate approach [to access control] consists in leaving the federation freely available to everybody (without any identification and authentication

procedure). Access control at the federation can in this case be enforced on the basis of the user's remote identity or of the site where the connection originated." This disclosure teaches that a user can log into the remote system using a user identification, then access the federated data without the transmission of the userid or password, but based only upon the site from which the request is made. This teaching, in combination with the other two cited references, clearly renders obvious the invention of at least the independent claims.

Furthermore, the Applicants cite a passage from section 3.2 as teaching that "Connection [to the federation] requires identification of the user and corresponding authentication of his identity by the federation." However, the Applicants fail to consider the footnote of the very next sentence, which reads "Note that this assumption does not rule out the possibility of anonymous connection. Anonymous connection may be treated with a special user identifier, anonymous." This anonymous connection corresponds to the situation cited above, wherein the federation is available to everyone, but access control at the federation is based on the site where the connection originated.

The Applicants' attention is also drawn to Table 1 (page 89), which discloses that one solution to access control at the federation is to use the identity of the remote site from which the request originated.

42. In response to the Applicants' arguments regarding claim 2, **Garrison** teaches a data processing environment including a security profile corresponding to a site (see paragraph 18 above). This is the security profile referred to in the rejection of claim 2 (paragraph 22 above). As stated in the rejection, **Yoshimoto** teaches the fact that the security profile is site specific. All of



this is clearly stated in the rejection of claim 1. However, since there is still evidently some confusion, the examiner has changed the wording of the rejection to more explicitly explain which reference teaches which limitation.

43. In response to the Applicants' arguments regarding claims 3, 8, 12, 13 and 18, the examiner respectfully responds that there was no admission that **Garrison** does not teach a "security profile corresponding to a site". This limitation, as stated in paragraph 13 of the previous Office action, and repeated in paragraph 18 above, is taught at col. 6, line 60 through col. 7, line 32, and also at col. 7, line 50 through col. 8, line 37.

The admission that is presumably being referred to by the Applicants is that **Garrison** does not teach a data processing environment wherein the security profile is site-specific. In other words, **Garrison** teaches a security profile that corresponds to a site (for which *any* security profile would qualify, since it must be implemented at *some* site), but not necessarily one that is specific to a site such that it can be used to differentiate between different sites.

44. In response to the Applicants' arguments regarding the rejection of claims 5, 9, 10, 15, 19 and 20 based in part on the **King** reference, the examiner responds that the data processing system as claimed comprises in part a database management system. **King** teaches that it is advantageous to choose MAPPER as the database management system because it is extremely versatile and is considered on the best fourth generation programs. Given this teaching, it would have been obvious to one of ordinary skill in the art at the time of the invention to choose MAPPER as the database management system for the claimed data processing environment.

*Conclusion*

45. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.


In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 703-746-5658.

Customer Service for Tech Center 2100 can be reached during regular business hours at (703) 306-5631, or fax (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

  
Luke S. Wassum  
Art Unit 2177

lsw  
2 October 2003

  
JOHN BREENE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100